Amendments to the Claims:

Without prejudice, this listing of the claims replaces all prior versions and listings of the claims in the present application:

Listing of Claims:

1. (Currently Amended) A device for preventing pirated copies of computer programs for use with a computer, comprising:

input and output devices for bidirectional data exchange with the computer;

a first memory element containing a data file that is transferrable to the computer via the output device, the data file including a key uniquely identifying a licensed copy of the computer program; and

a second memory element into which data is writable by the input device;

wherein the first memory element and the second memory element are arranged on a memory chip, and

wherein the device is configured to erase the key from the first memory element upon a successful transfer of the data file so that a subsequent attempt to transfer the data file to another computer does not result in a transfer of the key to the other computer unless the key has been transferred back to the device from the computer which received the key.

2. (Previously Presented) The device according to claim 1, wherein the memory chip includes a ROM memory chip.

3. (Original) The device according to claim 2, wherein the memory chip is a nonvolatile semiconductor memory.

4. (Original) The device according to claim 1, wherein the input and output devices are adapted to a module port of the computer so that the input and output devices are insertable into the module port.

5. (Currently Amended) A method of preventing pirated copies of computer programs, comprising the steps of:

connecting a device to a computer for bidirectional data exchange, the device including input and output devices and first and second memory elements;

transferring a first data file containing a key from the first memory element of the device to the computer, the key uniquely identifying a licensed copy of the computer program; ~~and~~

copying a second data file containing an identifier from the computer to the second memory element of the device; and

erasing the key from the from the first memory element if the transfer of the first data file was successful so that a subsequent attempt to transfer the data file to another computer does not result in a transfer of the key to the other computer unless the key has been transferred back to the device from the computer which received the key.

6. (Original) The method according to claim 5, further comprising the step of entering into the computer an enable number encoded with the key.

7. (Original) The method according to claim 5, further comprising the step of transferring the key from the computer back to the connected device after checking the identifier.

8. (Currently Amended) A data carrier storing a computer program, the computer program being executable by entering the data carrier into a computer, the data carrier containing a key and an identifier, the key uniquely identifying a licensed copy of the computer program the computer program, upon execution, carrying out the following steps:

transferring a first data file containing the key from a first memory element of a device to the computer, the device further including input and output devices; and

copying a second data file containing the identifier from the computer to a second memory element of the device,

erasing the key from the first memory element upon a successful transfer of the data file so that a subsequent attempt to transfer the data file to another computer does not result in a transfer of the key to the other computer unless the key has been transferred back to the device from the computer.

9. (Previously Presented) The device of claim 1, wherein the key includes an electronic key.

10. (Previously Presented) The device of claim 1, wherein the data file is transferable to the computer so that the data file is stored on the computer.

11. (Previously Presented) The device of claim 1, wherein the data file is transferable to the computer so that the data file is removed from the device.

12. (Previously Presented) The device of claim 1, wherein the data file is transferable to the computer so that the data file is stored on the computer and removed from the device.

13. (Currently Amended) A method of preventing a pirated copy of a computer program, comprising:

determining whether a dongle is connected to a computer;

checking whether the dongle contains a correct computer identifier when the dongle is connected to the computer;

copying a key to the dongle when the dongle contains the correct computer identifier;

erasing the key in the computer; ~~and~~

erasing the computer identifier in the dongle; and

preventing an execution of the computer program on the computer if the key is erased on the computer.

14. (Previously Presented) The method of claim 13, further comprising:

checking whether the key is valid; and

copying a license number of a computer program to the dongle.

15. (Previously Presented) The method of claim 14, further comprising:

reading out the license number of the computer program;

reading out an enable number that is encoded;

decoding the enable number using the license number and the key; and

activating program modules of the computer program using the enable number.